ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18
Stylesheet Version v18.0

Title of Invention	RANDOMIZED MODULAR REDUCTION METHOD AND HARDWARE THEREFOR

Application Number: 10/781311
Confirmation Number: 4864
First Named Applicant: Vincent Dupaquis
Attorney Docket Number: ATM-244
Art Unit: 2131
Search string: (5077793 or 5144574 or 5373560 or 5479511 or 5513133 or 5724279 or 5764554 or 5793659 or 5870478 or 5954788 or 5999627 or 6088453 or 6091819 or 6175850 or 6366673 or 6466668 or 20020039418 or 20020143836 or 20020161810).pn.

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	5077793	1991-12-31	Falk et al.	A1	380	28
	2	5144574	1992-09-01	Morita	A1	364	746
	3	5373560	1994-12-13	Schlafly	A1	380	30
	4	5479511	1995-12-26	Naccache	A1	380	28
	5	5513133	1996-04-30	Cressel et al.	A1	364	754
	6	5724279	1998-03-03	Benaloh et al.	A1	364	746
	7	5764554	1998-06-09	Monier	A1	364	746
	8	5793659	1998-08-11	Chen et al.	A1	364	746
	9	5870478	1999-02-09	Kawamura	A1	380	30
	10	5954788	1999-09-21	Suh et al.	A1	708	491
	11	5999627	1999-12-07	Lee et al.	A1	380	30
	12	6088453	2000-07-11	Shimbo	A1	380	28
	13	6091819	2000-07-18	Venkatesan et al.	A1	380	28
	14	6175850	2001-01-16	Ishii et al.	A1	780	491
	15	6366673	2002-04-02	Hollmann et al.	A1	380	28

	16	6466668	2002-10-15	Miyazaki et al.	A1	380	30

US Published Applications

Note: Applicant is not required to submit a paper copy of cited US Published Applications

init	Cite.No.	Pub. No.	Date	Applicant	Kind	Class	Subclass
	1	20020039418	2002-04-04	Dror et al.	A1	380	28
	2	20020143836	2002-10-03	Ebergen et al.	A1	708	491
	3	20020161810	2002-10-31	Mellott et al.	A1	708	491

Signature

Examiner Name	Date
	6/28/07

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	RANDOMIZED MODULAR REDUCTION METHOD AND HARDWARE THEREFOR

Application Number : 10/781311

Confirmation Number: 4864

First Named Applicant: Vincent Dupaquis

Attorney Docket Number: ATM-244

Art Unit: 2131

Examiner:

Search string: (5210710).pn

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
	1	5210710	1993-03-11	Jimmy K. Omura	A1	364	746.1

Signature

Examiner Name	Date
	6/28/07

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicants: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Country	Class	Sub Class	Translation Yes	No
	AK							
	AL							
	AM							
	AN							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

CBZ	AO	*Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards* by Jean-Francois Dhem, Doctorate of Applied Sciences Thesis, Universite Catholique de Louvain, May 1998, pages 11-22.
CBZ	AP	*Implementing the Rivest Sharmi and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor* by Paul Barrett, Security Bulletin, Computer Security Ltd., August 1986.

EXAMINER: [signature]

DATE CONSIDERED: 6/28/07

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicants: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Country	Class	Sub Class	Translation Yes No
	AK						
	AL						
	AM						
	AN						

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

CF	AO	*Efficient Implementation*, Handbook of Applied Cryptography, 1997, Menezes, Oorschot, and Vanstone, pages 591-635.
CF	AP	*Architectural Tradeoff in Implementing RS* Processor by Fu-Chi Chang and Chia-Jiu Wang, ACM SIGARCH Computer Architecture News archive, Department of Electrical and Computer Engineering, University of Colorado at Colorado Springs, Colorado, Volume 30, Issue 1, March 2002.
	AQ	

EXAMINER	DATE CONSIDERED: 6/28/07

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicants: Vincent Dupaquis et al.	
	Filing Date: Feb. 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Publ. Date	Country	Class	Sub Class	Translation Yes	No
	AK							
	AL							
	AM							
	AN							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AO	J. Grossschadel, *the Chinese Remainder Theorem and Its Application in a High-Speed RSA Crypto Chip*, 11 December 2000, IEEE Comput. Soc., U.S., pages 384-393, XP010529836. ISBN 0-7695-0859-6.
	AP	K.C. Posch et al.,r Microprocessing and Microprogramming, Elsevier Science Publishers, BV, Amsterdam NL., Vol. 29, No. 3, October 1990, pages 177-184, XP000151455, ISSN: 0165-6074.

EXAMINER: [signature]

DATE CONSIDERED: 6/28/07

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449	Atty. Docket No. ATM-244	Serial No. 10/781,311
LIST OF PRIOR ART CITED BY APPLICANT	Applicant: Vincent Dupaquis et al.	
	Filing Date: February 18, 2004	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Grant Date	Name	Class	Sub Class	Filing Date
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						

FOREIGN PATENT DOCUMENTS

Examiner Initial*		Document Number	Grant Date	Country	Class	Sub Class	Translation Yes	No
	AJ							
	AK							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

CZ	AL	A. Bosselaers et al., "Comparison of Three Modular Reduction Functions", Advances in Cryptology/Crypto '93, LNCS 772, Springer-Verlag, 1994, pp. 175-186.
CZ	AM	C.H. Lim et al., "Fast Modular Reduction With Precomputation", preprint, 1999 (available from CiteSeer Scientific Literature Digital Library, 15 pages.
CZ	AN	J.F. Dhem, "Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards", doctoral dissertation, Université catholique de Louvain, Louvain-la-Neuve, Belgium, May 1998.

EXAMINER:	DATE CONSIDERED: 6/28/07

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.